

BUSINESS PARTNER AUTOMATION PROGRAM INFORMATION SECURITY PRE-IMPLEMENTATION CHECKLIST

SECOND-LINE BUSINESS PARTNER

BUSINESS PARTNER NAME				TELEPHONE NUMBER ()	
BUSINESS ADDRESS		CITY	STATE	ZIP CODE	SERVICE PROVIDER

USE THE NUMBER LISTED ON THIS CHECKLIST TO IDENTIFY THE NARRATIVE, DIAGRAM, FLOOR PLAN, OR SUBMITTED MATERIAL WHEN PUTTING YOUR PACKAGE TOGETHER. *Place this form on top of the completed package.*

To assure a secure environment is maintained, DMV requires administrative measures and minimum standards are met by the First-Line Business Partner Service Provider (FLBPSP) and their Second-Line Business Partner (SLBP). To ensure that DMV measures and standards are met prior to implementation the partners must provide the following information or documents:

GENERAL SECURITY INFORMATION

- ☐ 1. Provide one (1) copy each of the FLBPSP security policies and or the Information Security Program policies; user guide or processing manual; and guidelines or Training Manual(s) for physical and electronic access for SLBP staff authorized to work with DMV resources and assets.
- ☐ 2. Provide a description of the Business Partners' process(es) for identifying possible security incidents. Identify what procedures or process(es) are utilized to prevent further security violation(s) after they are found, and how a security violation is documented and reported to DMV.

RESOURCE AND ASSET PHYSICAL SECURITY

- ☐ 3. Provide a floor plan and a detailed narrative describing workstation and facility security. The documentation must include overall facility security and intrusion prevention, entry control measures, as well as detail regarding the area(s) where DMV resources and assets are used, or stored (permanent and working storage), and where electronic data manager workstations and printers are located. Include details regarding security control measures (*i.e., the location and descriptions of any safe(s) or file cabinet(s) used for DMV controlled and accountable items security; identify areas that are public and employee and authorized employees only; details regarding facility security measures (i.e., alarm or surveillance systems); and identify the locations of internal and external doors, window, and other openings and how they are secured*).

ACCESS SECURITY

- ☐ 4. Provide a narrative that details how users are IDENTIFIED, AUTHENTICATED, and AUTHORIZED access to DMV BPA processes, resources, and assets.

RETENTION AND DESTRUCTION SECURITY

- ☐ 5. Provide a narrative that details how DMV information resources are secured and kept private while retained or captured via any method and or medium (electronic or physical), fixed or portable.
- ☐ 6. Provide a narrative that details how DMV information resources and assets are rendered un-readable, un-useable, and un-recoverable after legitimate business use has ended or destruction is required.

DECLARATION STATEMENT

As the Authorized or Designated representative of: _____

BUSINESS NAME

I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

PRINTED NAME OF AUTHORIZED REPRESENTATIVE

SIGNATURE OF AUTHORIZED REPRESENTATIVE



DATE